Amendment

20071210.103.A.001

Between

Single Touch Interactive, Inc.

And

AT&T Services, Inc.

AMENDMENT NO. 1

AGREEMENT NO. 20071210.103.C

This Amendment, effective on the date when signed by the last Party ("Effective Date"), and amending Agreement No. 20071210.103.C, is by and between Single Touch Interactive, Inc., a Nevada corporation ("Supplier"), and AT&T Services, Inc., a Delaware corporation ("AT&T"), each of which may be referred to in the singular as a "Party" or in the plural as the "Parties."

WITNESSETH

WHEREAS, Supplier and AT&T entered into Agreement No. 20071210.103.C on April 11, 2008 (the "Agreement"); and

WHEREAS, Supplier and AT&T desire to amend the Agreement as hereinafter set forth.

NOW, THEREFORE, in consideration of the premises and the covenants hereinafter contained, the Parties hereto agree as follows:

1. Section 1.2, Scope of Agreement, shall be amended to include the following:

1.2 Scope of Agreement

c. Supplier will provide, implement and maintain, and allow AT&T and/or AT&T's customers ("Customers", "Customer" for singular) to utilize, promote and support an Abbreviated Dial Code ("ADC") Registry Program (patent pending), which Registry Program facilitates wireless and landline communication between Customer and its End Users concerning the End Users' pharmacy orders and other pharmacy-related business.
d. Supplier shall provide to AT&T the Material and Services described herein and in Appendices M and N and will comply with the terms and conditions herein and therein, subject to the terms and conditions of this Agreement and pursuant to and in conformance with Orders submitted by AT&T. In the event of any conflict between the terms herein and the terms of the Agreement, the terms herein will prevail.
e. If Supplier rejects an Order, Supplier shall give AT&T written notice stating Supplier's reasons for rejecting the Order and the modifications, if any, that would make the Order acceptable to Supplier. Supplier shall furnish Materials that conform strictly to the Specifications established under this Agreement. If Supplier is unable to tender conforming Material, Supplier shall not tender non-conforming Material; the Parties agree non-conforming tenders are not an accommodation to AT&T. All Delivery Dates are firm, and time is of the essence.

2. Section 3.28, Price, shall be deleted and replaced as follows:

3.28 Price

a. Supplier shall furnish Material and Services at the prices set forth in Appendix B, or pursuant to firm prices quoted by Supplier for such Material and Services, whichever prices are lower. The prices for all Material and Services in Appendix B are subject to increases or decrease by a writing signed by both Parties, but, if Supplier at any time makes a general price decrease, Supplier shall promptly notify AT&T in writing and extend such decrease to AT&T effective on the date of such general price decrease.

b. Supplier shall strive to proactively reduce its costs and corresponding prices for Material and Services as charged to AT&T by at least five percent (5%) each calendar year, through the use of improved processes, supply chain economies and other cost reduction methods.

3. Section 4.9 Labor Disputes, shall be added as follows:

4.9 Labor Disputes

a. In the event of a labor dispute between AT&T and the union(s) representing AT&T's employees, AT&T may exercise its right to modify the Scope of Work under the Order on immediate notice, including postponing, reducing, or terminating the services to be provided under the Order and due to be performed after the commencement of a labor dispute. AT&T acknowledges and agrees that the exercise of such right may result in a delay in the resumption of Services when requested by AT&T.
b. The rights and obligations of the Parties under this Section are in addition to, and not a limitation of, their respective rights under the Sections entitled "Amendments and Waivers" and "Force Majeure."

4. Section 5.0, AT&T Supplier Information Security Requirements (SISR), shall be added to the Agreement as follows:

5.0 AT&T Supplier Information Security Requirements (SISR)

Supplier shall comply with the requirements of Appendix "O" entitled "AT&T Supplier Information Security Requirements (SISR)."

5. Section 6.0, Execution of Agreements, shall be added to the Agreement as follows:

6.0 Execution of Agreements

5.1 Transmission of Original Signatures and Executing Multiple Counterparts

Original signatures transmitted and received via facsimile or other electronic transmission of a scanned document, (e.g., .pdf or similar format) are true and valid signatures for all purposes hereunder and shall bind the parties to the same extent as that of an original signature. This Agreement may be executed in multiple counterparts, each of which shall be deemed to constitute an original but all of which together shall constitute only one document.

6. Appendix B - Price(s), shall be amended to include section (i) as follows:

Appendix B - Price(s)

(i) Once Supplier verifies a unique ADC (#XXX) is available on US mobile carriers including, but not limited to, AT&T Mobility, Verizon Wireless, Sprint, T-Mobile, Alltel, Leap Wireless and Customer orders the ADC, Supplier will grant Customer the right to use the ADC in accordance with the terms of this Agreement.

(j) Outbound off the IVR fee: AT&T shall pay Supplier an amount equal to the number of minutes used for the month multiplied by the per minute fee as outlined below corresponding to the minutes used for the calendar month that originate from an ADC and terminate outside the IVR. The call fee includes carrier airtime.

Total minutes per calendar month	per minute fee (Supplier to charge AT&T)
Less than 100,000	[Omitted]
100,001 to 1,000,000	[Omitted]
1,000,001 to 20,000,000	[Omitted]
20,000,001 to 50,000,000	First minute of each call: [Omitted] Additional minutes of each call: [Omitted]
Over 50,000,001	First minute of each call: [Omitted] Additional minutes of each call: [Omitted]

(k) In the event that AT&T and Supplier intend to include packaged messages for a particular offering the Text Message fee must be agree to between the parties in an Order, the parties agree to use the following format to include in the Order:

Text Message fee for packaged messages: AT&T shall pay to Supplier XXX dollars ($XXX), the "Monthly Minimum", for text message fee for packaged messages, according the table below corresponding to the number of messages sent or received by End Users or Customer and delivered to/from the wireless carriers during the calendar month. For the avoidance of doubt, the messages are not free for End Users. Wireless carriers fees will apply. Individual messaging packages shall be determined in each Order or Statement of Work.

Total messages per month	Per message fee
Less than or equal to XXX	$XXX per month(Monthly Minimum)
Between XXX, 001 to X,000,000	$.XX per message
Over X,000,001	$.XX per message

The terms and conditions of Agreement No. 20071210.103.C in all other respects remain unmodified and in full force and effect.

IN WITNESS WHEREOF, the Parties have caused this Amendment to Agreement No. 20071210.103.C to be executed as of the date the last Party signs.

Single Touch Interactive, Inc.	**AT&T Services, Inc.**
By: /s/James Darcey	By: /s/Anthony Cohen
Printed Name: James Darcey	Printed Name: Anthony Cohen
Title: SVP	Title: Senior Contract Engineer
Date: March 20, 2009	Date: March 20, 2009

Appendices

Appendix M – Intellectual Property Rights

1. Intellectual Property Rights

The Parties acknowledge that information transmitted between Customers and End Users utilizing the ADC registry program ("ADC Data") may be protected health information, as that term is defined in the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations (collectively, "HIPAA"), and that Supplier agrees to the provisions set forth in Appendix N, **HIPAA TERMS,** in this Agreement with respect to the ADC Data. No rights of any kind are granted or implied to Supplier with respect to the ADC Data other than those set forth herein.

2. Scope of Work

Supplier will provide, implement and maintain, and allow AT&T and/or Customer to utilize, promote and support an Abbreviated Dial Code ("ADC") Registry Program (patent pending), which Registry Program facilitates wireless and landline communication between Customer and its End Users.

3. Message Notification Service

To support this project, Supplier will accept transmission of XTML data from Customer for transmission to its End User. Supplier will compile an SMS, IVR, or email message according to Customer's pre-established guidelines and transmit this message to Customer's End Users as directed by Customer. Supplier will use carriers as they become available for this solution, to transmit this message.
All data coming from Customer to Supplier will be pushed to Supplier according to mutually-agreed upon data transmission standards. Supplier will pull no data from Customer. The circuit(s) between Customer and Supplier for transmission of the data to Customer (for retransmission to the End Users) and the retrieval of data coming back from the End Users by Customer from Supplier, will be maintained and operated by Customer. All routers, circuit, firewall, security, connection, and other issues related to this circuit(s) are the responsibility of Customer. Customer will maintain a secure VPN connection between the Customer database and the Supplier database. All security issues related to this VPN are the responsibility of Customer. All data communication for the delivery of these messages between Supplier and Customer will be initiated by Customer unless it is a response to a Customer initiated message. Customer will pull transmissions from Supplier's database coming back from the End Users. Customer will pull a copy of all data sent by Supplier.

Supplier will provide mirrored databases and transmission facilities for transmission of Customer's messages in separate data centers that are geographically redundant. Supplier will connect these data centers for mirroring purposes by private dedicated circuit connections and not via the public Internet.

4. Schedule of Fees

For fees refer to Appendix B of this Agreement.

Appendix N

HIPAA TERMS

This Health Insurance Portability and Accountability Act (HIPAA) Exhibit ("Exhibit") supplements and is made a part of this Agreement.

RECITALS

A. Supplier understands and acknowledges that Customer and its affiliates are a "Covered Entity" as defined by HIPPA and Supplier acknowledges and agrees that this Agreement creates a business relationship pursuant to which Supplier may have access to certain information disclosed by Customer or its End Users, some of which may constitute Protected Health Information (as defined below).

B. Supplier agrees to protect the privacy and provide for the security of Protected Health Information to which it has access pursuant to this Agreement in compliance with the Health Insurance Portability and Accountability Act of 1996, Public Law No. 104-191 ("HIPAA"), regulations promulgated there under by the U.S. Department of Health and Human Services (the "HIPAA Regulations"), and other applicable state and federal laws.

C. The purpose of this Exhibit is to satisfy certain standards and requirements of HIPAA, the Privacy Rule (as defined below), including, but not limited to, the contract requirements of 45 CFR Section 164.504(e), and the Security Rule (as defined below).

In consideration of the mutual promises below and the exchange of information pursuant to this Exhibit, Parties agree as follows:

1. Definitions.
   a. "Designated Record Set" shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 CFR Section 164.501.
   b. "Electronic Protected Health Information" (or "Electronic PHI") means Protected Health Information which is transmitted by Electronic Media (as defined in the Security and Privacy Rule) or maintained in Electronic Media.
   c. "Individual" shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 CFR Section 160.103 and shall include a person who qualifies as a Personal Representative in accordance with 45 CFR Section 164.502(g).
   d. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Part 164, Subparts A and E.

e. "Protected Health Information" (or "PHI") shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 CFR Section 160.103, as applied to the information created or received by Supplier from or on behalf of Covered Entity.
f. "Required by Law" shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 CFR Section 164.103.
g. "Secretary" shall mean the Secretary of the Department of Health and Human Services or his or her designee.
h. "Security Rule" shall mean the Security Standards for the Protection of Electronic Protected Health Information at 45 CFR Parts 160 and 162, and Parts 164, Subparts A and C.

2. Permitted Uses and Disclosures of PHI. Except as otherwise limited in this Exhibit, Supplier may use and disclose PHI solely: (i) to perform functions, activities, or services for, or on behalf of, Customer as specified in this Agreement, provided that such use or disclosure would not violate state law or the Privacy Rule if done by Customer; and (ii) for the proper management and administration of Supplier, or to carry out the legal responsibilities of Supplier. PHI may not be used in any other manner, whether individually, collectively, or in any compilation, statistical summary, or de-identified form, nor may it be disclosed to any third party without the express written consent of Customer or as Required by Law.

3. Obligations of Supplier. Supplier agrees to use and disclose PHI only as permitted or required by this Exhibit or as otherwise Required by Law. Supplier shall obtain reasonable assurances from any person to whom PHI is disclosed that it will remain confidential and will be used or further disclosed only as Required by Law or for the purpose for which it was disclosed to the person (which purpose must be consistent with the limitations imposed upon Supplier pursuant to this Exhibit), and that the person agrees to notify Supplier of any instances of which it is aware in which the confidentiality of the information has been breached.

a. Appropriate Safeguards. Supplier shall use appropriate safeguards to prevent use or disclosure of PHI by Supplier or its agent other than as provided for by this Exhibit. Supplier shall maintain a comprehensive written information privacy and security program appropriate to the size and complexity of Supplier's operations and the nature and scope of its activities. Any access to PHI by an unauthorized person, or by an authorized person for an unauthorized purpose, that results notwithstanding Supplier's substantial compliance with the terms of this Addendum, shall not be considered a violation of Supplier's obligations under this Exhibit.

b. Safeguards of Electronic PHI. Supplier shall implement and maintain appropriate administrative, technical and physical safeguards that reasonably and appropriately protect the authenticity, confidentiality, integrity, and availability of Electronic PHI that it creates, receives, maintains, or transmits. Moreover, Supplier and its agents shall keep all security measures current (for purposes of this provision, security measures shall be considered current if the current or previous major release of commercially-available software is installed on the equipment used to

provide the Services. Supplier's administrative, technical, and physical safeguards shall be implemented through written policies, procedures or guidelines, as reasonable and appropriate

c. Reporting of Improper Use or Disclosure. Supplier shall report to AT&T any use or disclosure of PHI not provided for by this Exhibit within two (2) days of becoming aware of such use or disclosure. Commencing on the compliance date of the Security Rule, Supplier shall report to AT&T any Security Incident within two (2) days of becoming aware of such incident. "Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system used to store or process Electronic PHI.

d. Supplier's Agents. Supplier shall ensure that any agent, to whom it provides PHI or Electronic PHI agrees to the same restrictions and conditions that apply through this Exhibit to Supplier, and agrees to implement reasonable and appropriate safeguards to protect such information. If any agents of Supplier are not subject to the jurisdiction or laws of the United States, or if any use or disclosure of PHI in performing services under the Agreement will be outside of the jurisdiction of the United States, such entities must agree by written contract with the Supplier to be subject to the jurisdiction of the Secretary, the laws, and the courts of the United States, and waive any available jurisdictional defenses as they pertain to the parties' obligations under this Agreement, the Privacy Rule, or the Security Rule.

e. Access to PHI. While it is not anticipated that Supplier will maintain PHI in a Designated Record Set, were that to occur, Supplier shall provide access (at the request of AT&T, and in the time and manner designated by AT&T) to PHI in a Designated Record Set, to AT&T or, as directed by AT&T, to an Individual in order to meet the requirements under 45 CFR Section 164.524. Section 3(e) will not apply with respect to services that do not include the retention of PHI by Supplier or its agent, or that include such retention of PHI for only a short period of time.

f. Amendment of PHI. While it is not anticipated that Supplier will maintain PHI in a Designated Record Set, were that to occur, Supplier shall make any amendment(s) to PHI in a Designated Record Set that AT&T directs or agrees to pursuant to 45 CFR Section 164.526, at the request of AT&T or an Individual, and in the time and manner designated by AT&T. If an Individual requests an amendment of PHI directly from Supplier or its agents, Supplier must notify AT&T in writing within two (2) days of receiving such request. Any denial of amendment of PHI maintained by Supplier or its agents shall be the responsibility of AT&T. This section will not apply with respect to services that do not include the retention of PHI by Supplier or its agent, or that include such retention of PHI for only a short period of time.

g. Documentation of Disclosures. Supplier agrees to document disclosures of PHI and information related to such disclosures as would be required for AT&T to respond to a request by Customer or an Individual for an accounting of disclosures of PHI in accordance with 45 CFR Section 164.528. At a minimum, such information shall include: (i) the date of disclosure; (ii)

the name of the entity or person who received PHI and, if known, the address of the entity or person; (iii) a brief description of the PHI disclosed; and (iv) a brief statement of the purpose of the disclosure that reasonably informs the Individual of the basis for the disclosure, or a copy of the Individual's authorization, or a copy of the written request for disclosure.

h. Accounting of Disclosures. Supplier agrees to provide to AT&T information collected in accordance with this section of this Exhibit to permit AT&T to respond to a request by Customer by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR Section 164.528. It shall be Supplier's responsibility to prepare and deliver any such accounting requested.

i. Subject to Section 4(c), with respect to the Services performed by Supplier under this Agreement, Supplier will retain the PHI provided to it by Customer or AT&T for no more than 48 hours and the Parties agree that disclosures made pursuant to the terms of this Agreement in providing the Services are not disclosures that must be accounted for under Section 3(g) or accounted for under Section 3(h). With respect to any disclosures that occur during the time Supplier has custody and/or control of the PHI that would qualify under Section 3(g), if any, Supplier will provide to AT&T the information collected in accordance with Section 3(g) within two (2) days after Supplier becomes aware of the disclosures.

j. Governmental Access to Records. Supplier shall make its internal practices, books and records, including policies and procedures relating to (i) the use and disclosure of PHI received from, or created or received by Supplier on behalf of, Customer, and (ii) the implementation of security safeguards, available to the Secretary for purposes of the Secretary determining Customer's compliance with the Privacy Rule and the Security Rule.

k. Mitigation. Supplier agrees to mitigate, to the extent practicable, any harmful effect that is known to Supplier of a use or disclosure of PHI by Supplier in violation of the requirements of this Exhibit.

l. Minimum Necessary. Supplier (or its agents) shall only request, use and disclose PHI in accordance with the terms of this Exhibit.

4. Term and Termination.

   a. Termination for Cause. Upon AT&T's knowledge of a material breach by Supplier of any of the obligations in this Appendix N, AT&T shall either (i) provide an opportunity for Supplier to cure the breach or end the violation within the time specified by AT&T, or (ii) immediately terminate this Amendment if cure is not possible. If cure or termination are not feasible, then AT&T shall report the violation to the Secretary.

   b. Effect of Termination.

(i) Except as provided in paragraph (ii) of this Section 4(b), upon termination of this Agreement for any reason, Supplier shall return or destroy all PHI received from Customer or AT&T, or created or received by Supplier on behalf of AT&T or Customer, and shall retain no copies of the PHI. This provision shall apply to PHI that is in the possession of agents of Supplier.

(ii) In the event that Supplier determines that returning or destroying the PHI is infeasible, Supplier shall provide to AT&T notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the parties that return or destruction of PHI is not feasible, Supplier shall extend the protections of this Amendment to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Supplier maintains such PHI.

5. Regulatory References. A reference in this Amendment to a section in the Privacy Rule or the Security Rule means the section as in effect or as amended, and with which Customer is required to comply.

6. Amendment. Should any provision of HIPAA or its implementing regulations be amended such that it materially alters the Parties' obligations under this Agreement, the Parties agree to negotiate in good faith mutually agreeable amendments as are necessary for Customer to comply with the requirements of the Privacy Rule, the Security Rule, and HIPAA.

7. Survival. The respective rights and obligations of Supplier under Section 4(b) of this Appendix N shall survive the termination of the Agreement.

8. Indemnification. In addition to, and not in limitation of, any indemnification rights of either Party in the Amendment or Agreement, Supplier shall defend, hold harmless, and indemnify AT&T including without limitation, its officers, directors, employees, agents, representatives and independent contractors ("Indemnified Parties"), from and against any and all third-party claims, actions, demands, liabilities, losses, damages, costs and expenses, including reasonable attorney's fees (collectively "Claims"), incurred as a result of Supplier's violation of the Privacy Rule, the Security Rule, or this Appendix N.

9. Definitions. Regulatory citations in this Exhibit are to the United States Code of Federal Regulations Title 45 Parts 160 through 164, as interpreted and amended from time to time by Health and Human Services (HHS), for so long as such regulations are in effect. Unless otherwise specified in this Agreement, all capitalized terms not otherwise defined shall have the meaning established for purposes of Title 45 Parts 160 through 164, as amended from time to time.

Appendix O - Security Attachment (SISR)

AT&T Supplier Information Security Requirements V3.6 (July 2008)

The following AT&T Supplier Information Security Requirements ("Security Requirements") apply to Supplier, its subcontractors, and each of their employees and/or temporary workers, contractors, vendors and/or agents who perform Services for, on behalf of, and/or through AT&T (for the purpose of this Appendix, each or all "Supplier") that include **any** of the following**:**

1. Supplier's performance of Services that involve the collection, storage, handling, or disposal of AT&T confidential Information;
2. Supplier-offered or -supported AT&T branded services using non-AT&T network and computing resources;
3. Connectivity to AT&T non-public networks and computing resources;
4. Custom software development or software implementation; or
5. Website hosting and development for AT&T and/or AT&T's customers.

Supplier shall be fully compliant with these Security Requirements prior to the performance of any such Services.
Supplier represents and warrants that during the term of this Agreement and thereafter (as applicable with respect to Supplier's obligations under the Survival of Obligations clause) Supplier is, and shall continue to be, in compliance with its obligations as set forth herein. In addition to all other remedies specified in the Agreement, Supplier agrees that AT&T shall be entitled to seek an injunction, specific performance or other equitable relief and be reimbursed the costs (including reasonable attorney's fees) by Supplier to enforce the obligations in these Security Requirements, including those that survive Termination, Cancellation or expiration of this Agreement. The provisions of this Appendix shall not be deemed to, and shall not, limit any more stringent security or other obligations of the Agreement.

Definitions:
Unless otherwise set forth or expanded herein, defined terms shall have the same meaning as set forth in the main body of the Agreement.
"Information Resources" means any systems, applications, and network elements, and the information stored, transmitted, or processed with these resources in conjunction with supporting AT&T and/or used by Supplier in fulfillment of its obligations under this Agreement.

"Sensitive Personal Information" or "SPI" means any information that could be used to uniquely identify, locate, or contact a single person (or potentially be exploited to steal the identity of an individual, commit fraud or perpetuate other crimes). Examples of SPI include, but are not limited to, social security numbers, national-, state- or province-issued identification number, drivers license numbers, dates of birth, bank account numbers, credit card numbers, and other credit related information, PINs, passwords, passcodes, password hint answers, Protected Health

Information as defined by the Health Insurance Portability and Accountability Act (HIPAA), biometric data, digitized signatures, and background check details.

In accordance with the foregoing, Supplier shall:

System Security
1. Actively monitor industry resources (*e.g.*, pertinent software vendor mailing lists and websites) for timely notification of all applicable security alerts pertaining to Supplier networks and computers.
2. Scan externally-facing systems with applicable industry standard security vulnerability scanning software (including, but not limited to, network, server, and application scanning tools) at a minimum monthly.
3. Scan internal systems with applicable industry standard security vulnerability scanning software (including, but not limited to, network, server, application and database scanning tools) at a minimum monthly.
4. Upon AT&T's request, furnish to AT&T its most current scanning results for those resources used to support AT&T.
5. Deploy one or more Intrusion Detection Systems (IDS) in an active mode of operation.
6. Remediate security vulnerabilities, including, but not limited to, those discovered through industry publications, vulnerability scanning, virus scanning, and the review of security logs, and apply applicable security patches in a timely manner, according to the following minimum guidelines: If: • A vulnerability exists and attack is underway: Supplier shall work on remediating/patching 24x7 • A vulnerability exists and attack is determined to be imminent: Supplier shall remediate/patch within seven (7) days. • A vulnerability exists and attack is determined to not be imminent: Supplier shall remediate/patch within thirty (30) days. All other security patches shall be applied within sixty (60) days.
7. Assign security administration responsibilities for configuring host operating systems to specific individuals.
8. Ensure that its security staff has reasonable and necessary experience in information/network security.
9. Ensure that all of Supplier's systems are and remain 'hardened' including, but not limited to, removing or disabling unused network services (*e.g.*, finger, rlogin, ftp, simple TCP/IP services) and installing a system firewall, TCP Wrappers or similar technology.
10. Change all default account names and/or default passwords in accordance with password requirements as set forth within requirement number 34, below.
11. Limit system administrator/root (or privileged, super user, or the like) access to host operating systems only to individuals requiring such high-level access in the performance of their jobs.
12. Require system administrators to restrict access by users to only the commands, data and systems necessary to perform authorized functions.
Physical Security
13. Ensure that all of Supplier's networks and computers are located in secure physical facilities with access limited and restricted to authorized individuals only.

14. Monitor and record, for audit purposes, access to the physical facilities containing networks and computers used in connection with Supplier's performance of its obligations under the Agreement.

Network Security
15. Separate AT&T's Information from the Internet and the destination web servers with a perimeter security gateway (*e.g.,* firewall). For additional clarification of this requirement, see the diagram below; however, the written requirements shall control with respect to the interpretation of this provision. [OMITTED GRAPHIC]
16. Upon AT&T's request, provide to AT&T a logical network diagram detailing the Information Resources (including, but not limited to, firewalls, servers, etc.) that will support AT&T.
17. Have a documented process and controls in place to detect and handle unauthorized attempts to access AT&T Information.
18. Use the strongest commercially available encryption technologies (minimum 256-bit encryption) for the transfer of AT&T Information outside of AT&T-controlled facilities and network. This also applies to electronically transmitted email communications containing AT&T Information.
19. Use strong authentication (*e.g.*, two factor token or digital certificates) for remote access.
Information Security
20. Not co-locate AT&T's application/Information on the same physical servers with any other customer's or Supplier's own application/information.
21. Have a documented procedure for the secure backup, transport and storage of AT&T Information and upon AT&T's request, provide such documented procedure to AT&T.
22. Maintain and, upon AT&T's request, furnish to AT&T a business continuity plan that ensures that Supplier can meet its contractual obligations under the Agreement, including the requirements of any applicable Statement of Work or Service Level Agreement.

23. Store AT&T SPI using the strongest commercially available encryption technologies (minimum 256-bit encryption). Sensitive data elements include, but are not limited to, Personally Identifiable Information.
24. Limit access to AT&T Information, including, but not limited to, paper hard copies, only to persons or systems authorized by AT&T under written agreement.
25. Be compliant with any applicable government- and industry-mandated information security standards including, but not limited to, the Payment Card Industry- Data Security Standards (PCI), National Automated Clearing House Associates (NACHA) Rules, Electronic Data Interchange (EDI), and HIPAA.
26. Return, or, at AT&T's option, destroy all AT&T Information, including electronic and hard copies, within thirty (30) days after the sooner of: (a) expiration or Termination or Cancellation of the Agreement; (b) AT&T's request for the return of Information; or (c) the date when Supplier (or its suppliers or representatives) no longer needs the Information. In the event that AT&T approves destruction as an alternative to returning the Information, then Supplier shall certify the destruction (*e.g.*, degaussing, overwriting, performing a secure erase, performing a chip erase, shredding, cutting, punching holes, breaking, etc) as rendering the Information non-retrievable.
27. Unless otherwise instructed by AT&T, when collecting, generating or creating Information for, through or on behalf of AT&T or under the AT&T brand, Supplier shall use the following AT&T proprietary marking: "**AT&T Proprietary Information (Internal Use Only)** Not for use or disclosure outside the AT&T companies except under written agreement"
Identification and Authentication
28. Assign unique UserIDs to individual users.
29. Have and use a documented UserID Lifecycle Management process including, but not limited to, procedures for approved account creation, timely account removal, and account modification (*e.g.,* changes to privileges, span of access, functions/roles) for all applications and across all environments (*e.g.,* production, test, development, etc.).
30. Enforce the rule of least privilege (*i.e.,* limiting access to only the commands and Information necessary to perform authorized functions according to one's job function).
31. Limit failed login attempts to no more than six (6) successive attempts and lock the user account upon reaching that limit. Access to the user account can be reactivated subsequently through a manual process requiring verification of the user's identity or, where such capability exists, can be automatically reactivated after at least three (3) minutes from the last failed login attempt.
32. Terminate interactive sessions that have been inactive for a designated period of time, not to exceed fifteen (15) minutes.
33. Require password expiration at regular intervals not to exceed ninety (90) days.

34. Use an AT&T-approved authentication method based on sensitivity of Information. When passwords are used, they must meet these requirements:
    - Passwords must be a minimum of six (6) characters in length.
    - Passwords must contain characters from at least two (2) of these groupings: alpha, numeric, and special characters.
    - Password construction must be complex and not contain names, dictionary words, combinations of words, or words with substitutions of numbers for letters, *e.g.*, s3cur1ty.
    - Passwords must not contain repeating or sequential characters or numbers.
    - Passwords must not contain sequences of three (3) or more characters from the UserID or system name.
    - The new password must not contain sequences of three (3) or more characters from any of the previous four (4) passwords.
    - Passwords must not contain a sequence of two (2) or more characters more than once, *e.g.*, a12x12.

    Note: Applications housing more sensitive Information, as identified by AT&T, may require an authentication mechanism stronger than passwords and the authentication mechanism must be approved by AT&T in advance in writing. Examples of stronger authentication methods include tokens, digital certificates, passphrases, and biometrics.

35. Use a secure method for the conveyance of authentication credentials (*e.g*. passwords) and authentication mechanisms (*e.g*. tokens or smart cards).

Warning Banner

36. Display a warning or "no-trespassing" banner on applicable login screens or pages when in Supplier's environment and not an AT&T branded product or service.
    (example long version):

    This is an <company name> system, restricted to authorized individuals. This system is subject to monitoring. Unauthorized users, access, and/or modification will be prosecuted.

    (example short version):

    <company name> authorized use ONLY, subject to monitoring. All other use prohibited

    For AT&T branded products or services or for software developed for AT&T, Supplier shall display a warning banner on login screens or pages provided by AT&T.

Software and Data Integrity

37. Have current antivirus software installed and running to scan for and promptly remove viruses.
38. Separate non-production systems and data from production systems and data.
39. Have a documented software change control process including back out procedures.

40. Have database transaction logging features enabled and retain database transaction logs for a minimum of six (6) months.
41. For all software developed, used, furnished and/or supported under this Agreement, review such software to find and remediate security vulnerabilities during initial implementation and upon any modifications and updates.
42. Perform quality assurance testing for the application functionality and security components (*e.g.*, testing of authentication, authorization, and accounting functions, as well as any other activity designed to validate the security architecture) during initial implementation and upon any modifications and updates.
Privacy Issues
43. Restrict access to any AT&T SPI to authorized individuals.
44. Not store AT&T SPI on removable media (*e.g.*, USB flash drives, thumb drives, memory sticks, tapes, CDs, external hard drives) except for backup purposes as required under contract and using the strongest commercially available encryption technologies (minimum 256-bit encryption).
Monitoring and Auditing Controls
45. Restrict access to security logs to authorized individuals.
46. Review, on no less than a weekly basis, security logs for anomalies and document and resolve all logged security problems in a timely manner.
47. Retain complete and accurate records relating to its performance of its obligations arising out of these Security Requirements and Supplier's compliance herewith in a format that will permit audit for a period of no less than three (3) years, or longer as may be required pursuant to a court order or civil or regulatory proceeding. Notwithstanding the foregoing, Supplier shall only be required to maintain security logs for a minimum of six (6) months. In the event Supplier is provided connectivity to AT&T, Supplier shall maintain logs of user sessions (including application to application sessions) relating to such connectivity. These session logs must include: login identification, user request records, system configuration, and timestamps and/or duration of access. These session logs must be retained for a minimum of six (6) months.
48. Upon AT&T's request for audit, Supplier shall schedule a security audit to commence within thirty (30) days from such request. In the event AT&T, in its sole discretion, deems that a security breach has occurred, Supplier shall schedule the audit to commence within one (1) day of AT&T's notice requiring an audit. This provision shall not be deemed to, and shall not limit any more stringent audit obligations permitting the examination of Supplier's records contained in this Agreement.
49. Within thirty (30) days of receipt of the audit report, provide AT&T a written report outlining the corrective actions that Supplier has implemented or proposes to implement with the schedule and current status of each corrective action. Supplier shall update this report to AT&T every thirty (30) days reporting the status of all corrective actions through the date of implementation. Supplier shall implement all corrective actions within ninety (90) days of Supplier's receipt of the audit report.
Reporting Violations

50. Have and use a documented procedure to follow in the event of an actual or suspected unauthorized intrusion or other security violation, including but not limited to, a physical security or computer security incident (*e.g.*, hacker or attempted hacker activity or the introduction or attempted introduction of a virus or malicious code), which includes immediate notification to the AT&T Computer Security Incident Response Team (ACSIRT). ACSIRT 24 hour contact information: • Phone: 1 866 466-2288, prompt 8 (U.S.) • Phone: 1 908 234-3327 (International)
51. Provide AT&T with regular status updates on any actual or suspected unauthorized intrusion or other security violation including, but not limited to, actions taken to resolve such incident, at four (4)-hour intervals (or at other mutually agreed intervals or times) for the duration of the incident, and within five (5) days of the closure of the incident, a written report describing the incident, actions taken by the Supplier during its response and Supplier's plans for future actions to prevent a similar incident from occurring.
Software Development and Implementation
52. Ensure, prior to furnishing or development of custom software, that such software incorporates applicable AT&T security requirements as provided by AT&T.
Security Policies and Procedures
53. Ensure that all personnel, subcontractors or representatives performing work on any AT&T Information Resources or the resources used to interconnect to AT&T resources or the resources used to house AT&T Information under this Agreement are in compliance with these Security Requirements.
54. Notify AT&T of any policy changes that could affect the security controls put in place to secure AT&T's Information.
55. At a minimum annually, review these Security Requirements to ensure that Supplier is in compliance with the requirements.
56. Return all AT&T owned or provided access devices (including, but not limited to, SecurID tokens, information storage devices, software, and/or computer equipment), as soon as practicable, but in no event more than fifteen (15) days after the sooner of: (a) expiration, Termination, or Cancellation of the Agreement; (b) AT&T's request for the return of such property; or (c) the date when Supplier (or its suppliers or representatives) no longer need such devices.

Connectivity Requirements

In the event Supplier has, or will be provided, connectivity (*e.g.*, access to AT&T's or its customers' networks) in conjunction with this Agreement, then in addition to the foregoing, the following Security Requirements shall apply to Supplier:

1. In the event a data connection agreement, such as a “Master Data Connection Agreement,” "Data Connection Agreement,” and/or “Connection Supplement” ("DCA") exists between the Parties, and incorporates this Agreement by reference, or is otherwise integrated with, or used to govern the Parties’ connectivity obligations under, this Agreement, such DCA is hereby superseded by the terms of the Security Requirements, effective as of the date these Security Requirements become effective under the Agreement, and the terms of such DCA are amended to require that the Security Requirements and not the DCA are controlling in the Agreement (as well as any agreements subordinate to this Agreement). Notwithstanding the foregoing, the DCA remains in full force and effect for all other agreements between the Parties to which it applies.

2. Supplier shall:
    a. Use only the AT&T Chief Security Office (CSO) approved facilities and connection methodologies to interconnect AT&T’s data facilities with Supplier’s data facilities and to provide access to the data for each connection.
    b. NOT establish interconnection to endpoint resources and/or end users outside the United States. Interconnections to endpoint resources and/or end users outside the United States require the express prior written consent of AT&T.
    c. Provide AT&T access to any Supplier facilities during normal business hours for the maintenance and support of any AT&T equipment (*e.g.,* router) used for the transmission of Information under this Agreement.
    d. Use any AT&T equipment provided under this Agreement only for the furnishing of those Services or functionalities explicitly defined in this Agreement.
    e. Ensure that all Supplier interconnections to AT&T pass through the designated AT&T perimeter security gateway (*e.g.,* firewall)**.**
    f. Ensure that Supplier interconnections to AT&T terminate at a perimeter security gateway (*e.g.,* firewall) at the Supplier end of the connection.

3. In addition to other rights set forth herein, AT&T shall have the right to:
    a. Gather information relating to access, including Supplier’s access, to AT&T networks, processing systems and applications. This information may be collected, retained and analyzed by AT&T to identify potential security risks without further notice. This information may include trace files, statistics, network addresses, and the actual data or screens accessed or transferred.
    b. Immediately suspend or terminate any interconnection if AT&T, in its sole discretion, believes there has been a breach of security or unauthorized access to or misuse of AT&T data facilities or Information.